Les transactions commerciales et industrielles par voie électronique :

Poullet, Yves

Published in:
Le droit des affaires en évolution : le juriste face à l'invasion informatique

Publication date:
1996

Document Version
le PDF de l'éditeur

LES TRANSACTIONS COMMERCIALES ET INDUSTRIELLES PAR VOIE ÉLECTRONIQUE

De quelques réflexions autour du droit de la preuve

PAR

Y. POULLET

DIRECTEUR DU CRID
PROFESSEUR À LA FACULTÉ DE DROIT ET AU DGTIC
(DES EN DROIT ET GESTION DES TECHNOLOGIES
DE L'INFORMATION ET DE LA COMMUNICATION)
FUNDP (NAMUR)

1. — *Un commerce sans papier.* L'utilisation couplée de l'ordinateur et des télécommunications autorise, dans les relations entre personnes, en particulier d'entreprises, un commerce sans papier (paperless trading). Avec le papier disparait aussi la griffe manuscrite à laquelle le droit reconnait la qualité de signature.

D'un ordinateur à l'autre, des données électroniques circulent. Elles prétendent établir, modifier ou annuler un contrat, adresser une facture ou accomplir une formalité administrative. Ces transactions commerciales autrefois limitées à des entreprises ayant des relations commerciales suivies se multiplient dans le cadre de réseaux aussi ouverts que ceux d'Internet. L'absence de relations préalables entre parties rend nécessaire plus encore qu'hier des procédures d'authentification des partenaires en présence et de protection des messages vis-à-vis des tiers. On note également que ces transactions se noueront par échange de textes, de voix ou d'images, là où traditionnellement, le droit de la preuve des contrats se focalisait sur les seuls documents textuels.

2. — *Une réflexion tripartite.* Notre propos est d'examiner quelques questions juridiques soulevées par ce commerce par voie électronique (1) et ce en trois parties.

— la première est préjudicielle. Elle étudie le cadre légal. Celui-ci peut-il reconnaître quelque valeur à la « signature » et à l'écrit électronique, la ou notre code civil réclame un acte sous seing privé ? Certes, des logiciels dits de cryptographie, des logiciels de contrôles, des certificateurs de message (2) enferment mieux qu'un coffre bancaire les messages d'ordinateur et rendent l'imitation d'une signature électronique plus difficile que celle d'une signature manuscrite. Certes, aux arguments de nécessité, s'ajoutent encore les arguments économiques (3) de bonne gestion des entreprises : le papier circule lentement, sa conservation est coûteuse mais même cumulés, ces arguments techniques et économiques convaincront-ils le juge, appelé à faire respecter la loi (4) ;

— la deuxième analyse la solution conventionnelle apportée par les « EDI model agreements » à diverses questions soulevées par les transactions électroniques ;

— enfin, la troisième aborde la solution institutionnelle qui, sans exclure les solutions légales et conventionnelles, se développe et tend à se généraliser : celle des « Trusted Third Parties » (T.T.P.) en d'autres termes des « tiers certificateurs », sorte de notaires (5) électroniques.

(1) Nous n'aborderons pas les questions particulières soulevées dans les relations entreprises-consommateurs lorsque l'ordinateur est utilisé pour l'offre, la commande voire la consommation de biens ou services. Ce point sera développé par le Prof. G. Ballon. Nous ne pourrons également aborder la question de la responsabilité des différents acteurs intervenant dans la conclusion d'une opération commerciale sans papier (A ce propos, le lecteur se réferera aux réflexions de X. THUNIS, *La responsabilité dans les transferts électroniques de fonds*, Thèse à paraître dans la collection des travaux de la Faculté de Droit de Namur, et à celles de E. MONTERO, *La responsabilité pour la fourniture de données en ligne*, thèse à paraitre dans la même collection.

(2) Sur les aspects techniques de la sécurité des transactions electroniques, lire notamment, Warwick FORD, *Computer Communication Security : Principles, Standards Protocoles and techniques (1994)*, Prentice Hall, New York.

(3) Sur la question du coût en particulier de l'archivage, les réflexions déjà anciennes de CHAMOUX, *La preuve dans les affaires*, LITEC, Paris, pp. 105 à 107.

(4) Sur le droit belge de la preuve, N. VERHEYDEN-JEANMART, *Droit de la preuve, Précis de la Faculté de Droit de l'UCL*, Larcier, Bruxelles, 1991.

(5) « Par certification, on entend toute technique utilisée par un tiers, qui présente par rapport aux deux parties à la transaction des conditions d'indépendance telles et qui a pris des mesures de sécurité telles que l'authenticité et l'intégrité du message peuissent être garanties en cas de contestation sur le contenu, le moment ou l'origine de celui-ci », M. ANTOINE, « La certification », *Rev. dr. Comm.*, 1, 1995, 4-14.

PREMIÈRE PARTIE. — LE CADRE LÉGAL ET LA RÉCEPTION DES PREUVES INFORMATIQUES

A. — *Le régime légal de la preuve face à l'informatique*

3. — *Des faits aux actes.* La preuve d'un fait juridique est libre. Ce principe constamment rappelé par notre doctrine et notre jurisprudence conduit à accepter la preuve à « caractère informatique ou télématique ». Certes, il restera à celui qui s'en prévaut à emporter la conviction du juge, en démontrant la qualité, la force probante de celle-ci. Une telle démonstration peut s'avérer difficile face à un juge « plus sensible » à la production d'un document tangible qui fait partie de son univers familier (6). Nous reviendrons sur ce point : le régime de la preuve libre n'est pas le régime du laisser faire complet.

La distinction entre acte et fait juridique n'est pas évidente : le paiement, soit l'exécution d'une obligation est un fait juridique du moins dans nos droits belge et français. En d'autres termes, par exemple, si le contrat d'abonnement à une banque de données est un acte juridique, les multiples interrogations qui peuvent avoir lieu dans le cadre de cet abonnement, pourraient être qualifiées de faits juridiques et bénéficier de ce fait du régime de la preuve libre (7).

4. — *Les actes : un régime strict.* L'acte juridique voit la preuve de sa conclusion et de son contenu soumis à un régime légal plus contraignant du moins en droit civil. Assorti d'exceptions (8), le régime de l'article 1341 du code civil complété par quelques dispositions (9) repose sur les principes suivants ;

(6) LAMY, *Droit de l'informatique*, éd. 1995, n° 2282.

(7) La même question pourrait se poser à propos des multiples opérations de retraits de fonds ou de dépôt de fonds accomplies dans le cadre d'un contrat de mise à disposition d'une carte bancaire. Ce dernier contrat doit-il s'analyser comme un contrat cadre suivi lors de chaque opération d'un contrat spécifique ou l'ensemble s'analyse-t-il comme un contrat unique de compte couplé avec une possibilité électronique d'activation ? Sur cette discussion, lire Y. POULLET, X. THUNIS, « Introduction aux aspects juridiques de la télématique », in *La Télématique, Aspects juridiques, économiques et socio-politiques*, T. 1, Gent, Story-Scientia, 1984, 125-191.

(8) Pour l'étude des articles 1347 et 1348 du code civil, l'auteur renvoie à l'ouvrage de N. VERHEYDEN déjà cité et à l'étude de M. ANTOINE, J.F. BRAKELAND et M. ELOY, « Le droit de la preuve face aux nouvelles technologies de l'information et de la communication », *Cahier du CRID*, n° 7, Story Scientia, 1991, 227 pages.

(9) Ainsi les articles 1325 et 1326 du code civil.

qu'apparemment contredit la preuve informatique ou télématique (10).

— le principe de la permanence du support auquel chacun doit pouvoir se référer, et que contredit la volatilité intrinsèque du document électronique ;
— le principe de la signature qui identifie et authentifie l'origine des auteurs de la transaction. La signature apparait comme leur expression personnelle, ce que ne peut constituer un code secret.
— le principe du contradictoire qui exige que chacun des contractants dispose à égalité les moyens de preuve. Il s'agit typiquement de la formalité du double prévue à l'article 1325 du code civil, formalité que heurte l'unilatéralité de la conservation des moyens de preuve, existante dans la plupart des systèmes d'information utilisés pour la conclusion de transactions par voie électronique (11).
— enfin, le principe de la transparence ou de lisibilité (12) : chacun doit être à même à travers le mode d'établissement de la convention de mesurer la portée de son engagement.

5. — *Les réticences face à la preuve électronique.* Le respect des principes ci-dessus énoncés est traditionnellement et idéalement assuré par le système de l'écrit papier et de la signature manuscrite dont la valeur repose tant sur une consécration populaire (13) que sur un arsenal répressif condamnant toute manipulation de l'écrit ou toute falsification de signature (14). C'est dans le cadre de cet ensemble culturel, social et réglementaire que doit se lire l'article 1341 du Code civil. Sans

(10) Comp. avec les critiques adressées par la rapport de Fr. Gallouedec-Genuys et alii, « Une société sans papier ?, Nouvelles technologies et droit de la preuve », *Doc. fr.*, 1990, p. 64 et 65.

(11) C'est en particulier cette unilatéralité qui conduit le juge Sétois dans l'affaire Credicas à rejeter toute valeur à la signature informatique : « il ne saurait y être supplé par ce que la société nomme 'signature informatique...' qui émane non de celle à qui on oppose mais d'une machine dont la demanderesse a la libre et entière disposition ».

(12) Comme le souligne en particulier la législation allemande. A ce propos, les réflexions de I. de Lamberterie, « La valeur probatoire des documents informatiques dans les pays de la CEE », *R.I.D.C.*, 1992, pp. 641 et s.

(13) A ce propos, les remarquables développements de J. Larrieu, « Les nouveaux moyens de preuve : pour ou contre l'identification des documents informatiques à des écrits sous seing privé ? », *Cahiers Lamy, Droit de l'Informatique*, I, 1988, pp. 30 et s. : « Il faut prendre en compte la dimension symbolique de l'écriture et de la signature ».

(14) L'article 1323 du Code civil permet le désaveu de l'écriture. Le code pénal réprime le faux en écriture et la destruction de l'écrit.

doute, ceci explique la réticence de nombre de juristes à l'acceptation d'une preuve électronique (15).

Certes, des exceptions légales existent par lesquelles des auteurs ont parfois voulu faire reconnaître les moyens électroniques de preuve. Certaines de ces exceptions apparaissent peu appropriées. L'impossibilité de prouver par écrit est une exception dont le maniement apparaît difficile, au moment où c'est volontairement que celui qui se prévaudrait de cette exception s'est privé d'un écrit (16) et la règle du commencement de preuve par écrit suppose un écrit (17). D'autres, sont plus appropriés : entre commerçants, la preuve n'est-elle pas libre et en définitive le régime légal de la preuve étant supplétif (18), une convention ne peut-elle soustraire l'opération télématique aux exigences de l'écrit sous seing privé ? Mais même ces exceptions sont d'un maniement délicat :

— le régime de liberté de la preuve, nous l'avons dit (*supra* n° 3) à propos des faits juridiques, laisse entière la charge de convaincre le juge de la valeur de la preuve électronique celle-ci une fois déclarée recevable. La recevabilité de tout moyen

(15) A preuve, ce propos d'un juge américain : « Ayant comme beaucoup d'autres citoyens reçu des factures informatisées pour des motifs payés depuis longtemps, je ne suis pas prêt d'accepter le produit de l'ordinateur comme la Sainte Ecriture », (Propos repris par MMs Amory et Poullet in *Le Droit de la preuve face à l'informatique et à la Télématique*, *R.I.D.C.*, 1985, p. 348).

(16) C'est par ce biais cependant que la loi française du 12 juillet 1980 a introduit la preuve informatique en reconnaissant la valeur de copie fidèle (à ce propos F. Chamoux, « La loi du 12 juillet 1980, une ouverture sur de nouveaux moyens de preuve », *J.C.P.*, 1981, II, n° 3008. Certes, dira-t-on, l'impossibilité peut, selon la doctrine (« De Page, *Traité de Droit civil*, n° 905), résulter d'un usage à condition, ajoute la jurisprudence, qu'il soit unanimement admis dans la région, comme une règle qui, à défaut de stipulation contraire, est applicable aux conventions de même nature et par suite comme une règle qui complète la volonté des parties ».

(17) Est considéré comme écrit « tout ce qui émane, sous une forme littérale quelconque, de la partie à qui on l'oppose », (Cass. 21 oct. 1891, *Pas.*, 1892, I, p. 58). Cf. également F. Chamoux, *La preuve dans les affaires*, Paris, LITEC, 1979, I, 24. L'interprétation de la notion d'« écrit » a parfois été plus large. Ainsi, on a parfois admis comme écrit, des enregistrements sonores ou les déclarations faites par des parties lors de comparutions personnelles en justice (cf. à ce propos, N. Verheyden, *op. cit.*, p. 168).

(18) Sur le caractère supplétif du droit de la preuve, la conclusion de l'étude de droit comparé PROBAT effectuée pour la DG XIII : « Il apparait dans tous les pays européens, qu'en règle générale, le droit de la preuve ne relève pas de l'ordre public et que les conventions de preuve sont en principe valables sauf dispositions expresses dans les textes législatifs » (I. De Lamberterie, « La valeur probatoire des documents informatiques dans les pays de la C.E.E. », *R.I.D.C.*, 1992, 3, p. 679). A propos de la validité de ces conventions mais également leurs limites, M. Boizard, « Preuve des paiements par cartes bancaires et signature informatique », *Cahiers Lamy, Droit de l'informatique*, 1988, pp. 10 et s., n^{os} 14 et s.

de preuve affirmée par l'article 25 du code de commerce laisse non résolue la question de sa force probante (19).

— la possibilité de dérogation conventionnelle a ses limites : premièrement elle ne vaut qu'entre les parties contractantes et suppose donc qu'un contrat préétabli selon les règles de l'article 1341 du code civil existe entre les parties, ce qui peut être difficile. En effet, se généralise l'utilisation des réseaux à des fins contractuelles même entre parties non préalablement en relations contractuelles (20). Secondement, les dérogations conventionnelles ont certaines limites et ne peuvent priver une partie de pouvoir s'y opposer en justice (21).

6. — *Le pari.* Plutôt que de légitimer la preuve électronique par le biais d'exceptions, notre propos dès 1992 a plutôt été de montrer qu'une approche ouverte et fonctionnelle des concepts du code civil permette de plaider pour reconnaître à certaines signatures électroniques, la qualité de signature et à certains documents électroniques, celle d'écrit et ce au plein sens juridique du terme.

Il ne peut être question de reprendre ici l'entiéreté du raisonnement mais simplement de le résumer et de l'étayer par de nombreux appuis extérieurs survenus depuis l'exposé de cette démarche.

En effet, cette approche dite de l'« équivalent fonctionnel » a reçu le support marqué des travaux de la CNUDI lors de l'élaboration de son « Guide pour l'incorporation de la loi type sur certains aspects juridiques de l'échange de données informatisées (EDI) et des moyens connexes de communications » (22).

(19) Comme le montre à suffisance les réflexions de la doctrine nordique à propos de leur système légal de preuve libre. A ce propos, lire tant l'article de M.B. ANDERSEN que celui de A. GALTUNG, *Evidential Issues in an EDI context according to Norvegian Law, Law, Computers & Artificial Intelligence*, 1, 3, 1992, pp. 345 et s.

(20) Sur cette limite, not., A. BENSOUSSAN, *La convention de preuve dans les accords d'interchange*, Lamy, Droit de l'Informatique, 1993, Suppl. n° 50, p. 9, C. XUEREF et P. BROUSS, *EDI des EDITERMS pour traiter les problèmes juridiques de l'EDI, propositions pour l'avenir*, DIT, 1992/3, p. 9.

(21) A ce propos, B. AMORY et Y. POULLET, *Les relations contractuelles banques-entreprises entourant la mise à disposition de services télématiques*, B.B. e Tit. di Cred., 1988, 378 à 380 ; cf. également l'article 32 de la loi belge sur les pratiques du commerce (*M.B.*, 29 août 1991) qui interdit la renonciation des consommateurs à se prévaloir *a priori* des moyens de preuve offerts par le droit civil.

B. — *La signature électronique*

7. — *Signature v. Signature électronique.* Traditionnellement la signature est définie comme étant un graphisme personnel qui permet d'établir la présence physique du souscripteur à l'acte et par lequel une personne manifeste son consentement. Elle a donc une double fonction : elle identifie l'auteur de l'acte et exprime sa volonté (23).

Le vocable de « signature électronique » est fréquemment utilisé, est-il acceptable juridiquement ? Certes, la jurisprudence de nombreux pays (Belgique, Danemark, Portugal, Allemagne) maintient l'exigence d'une signature manuscrite, marque par laquelle une personne révèle sa personnalité aux tiers. Une conception plus fonctionnelle de la signature s'écarte d'une vision aussi étriquée. Il s'agit d'un signe par lequel une personne, d'une part, s'identifie comme l'auteur d'un acte et, d'autre part, indique se volonté d'adhérer au contenu de l'acte auquel la signature se réfère et sur lequel elle a été apposée. En ce sens, certains procédés d'identification et d'authentification électroniques pourraient être reconnus comme de véri-

(22) A/CN.9/426-CNUDI, 29e session, New York, 28 mai-14 juin, 1996, nos 30 et s. Le rapport du secrétaire général s'exprime comme suit : « La loi type propose donc une nouvelle approche, parfois désignée sous l'appellation 'approche fondée sur l'équivalent fonctionnel', qui repose sur une analyse des objectifs et des fonctions de l'exigence traditionnelle de documents papier et vise à déterminer comment ces objectifs ou fonctions pourraient être assurés au moyen des techniques de l'EDI. Par exemple, un document papier assume notamment les fonctions suivantes : fournir un document lisible par tous ; fournir un document inaltérable ; permettre la reproduction d'un document de manière à ce que chaque partie ait un exemplaire du même texte ; permettre l'authentification des données au moyen d'une signature ; enfin, assurer que le document se présentait sous une forme acceptable par les autorités publiques et les tribunaux. Il convient de noter que pour toutes les fonctions du papier susmentionnées, les enregistrements électroniques peuvent garantir le même niveau de sécurité avec, dans la plupart des cas, une plus grande fiabilité et rapidité, notamment en ce qui concerne l'identification de la source et le contenu des données à condition qu'un certain nombre d'exigences techniques et juridiques soient respectées ». Cette démarche précisément fondait l'analyse proposée par M. ANTOINE et M. ELOY, « Le droit de la preuve face aux nouvelles technologies de l'information », Bruxelles, Story Scientia, *Cahier du CRID*, n° 9, 1992, pp. 64 et s.

(23) N. VERHEYDEN, *Droit de la preuve, Précis de la Faculté de Droit de l'UCL*, Larcier, Bruxelles, 1991, p. 234 ; cf. également, M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », *R.C.J.B.*, 1985, p. 69.

tables signatures (24) selon le principe de l'équivalent fonctionnel.

8. — *La signature électronique* (25). **Un bref aperçu technique.** « Le terme authentification : écrit J. Hubin (26), est utilisé dans deux contextes différents. L'authentification de documents est le mécanisme qui permet de s'assurer qu'un document a bien été émis par une personne autorisée (authentification de l'origine) et qu'il n'a subi aucune modification (authentification du contenu). Un document peut prendre deux formes différentes : il s'agit d'un message émis sur un réseau ou d'un fichier stocké sur un support quelconque. L'authentification d'un acteur consiste à s'assurer de la 'véritable' identité de l'auteur ».

La notion de signature électronique s'adresse à cette seconde forme, encore que, et nous le verrons, les procédures de cryptographie permettent d'assurer tout à la fois l'authentification de l'auteur et du document.

L'authentification de l'auteur se réalise par diverses méthodes : la plus courante est celle par les connaissances, en d'autres termes, la certitude relative à l'auteur du message vient du fait que seul cet acteur connaît l'information qui permet au destinataire du message de la reconnaître, ainsi un mot

(24) Comp. avec les conclusions de Andersen en droit danois, droit basé sur la liberté de preuve : « It is however generally held that a digital signature could be equalled with a written signature under circumstances where thre would generally be a high degree of certainly that it aron from the person in question and reflected his intent to be bound by the digitally signed document » (M.B. ANDERSEN, *The legal status and effect of digital signatures*, paper presented to the Worldwide Electronic Commerce, Conference, Maryland, october 20, 1995).

Plus clairement encore, l'affirmation du Comité ayant présidé à la révision de la loi de l'Utah sur la signature (*EDI Law Rev.*, 1995, p. 158). « Since, as the appendix explains, a digital signature is the functional equivalent of a paper signature... » et la déclaration de H.H PERRITT (The Electronic Agency and the Traditional Paradigms of Adm. Law, 44 Adm. Law Rev., 79 [1992]). « The concern with electronic signatures is a red herring. A variety of techniques for authentificating electronic documents exists that are a good as better than traditional handwritten signatures — There is growing agreement that authentification and signature concerns can be addressed by existing legal concepts in conjunction with adequate audit and recordkeeping controls ».

(25) Nous ne pouvons ici être complet. Nous renvoyons le lecteur sur ce point à l'ouvragre magistral de J. HUBIN, « La sécurité informatique », *Cahier du CRID*, n° 13, à paraître, Story Scientia, Bruxelles, 1996, en particulier pp. 60 et s. Cf. pour d'autres références l'imposante bibliographie reprise par M. J. HUBIN et le rapport de l'Office of Technology Assessment (O.T.A.) remis à l'U.S. Congres, *Issue update on Information, Security and Privacy in Networks Environments*, Washington, D.C., 1995.

(26) J. HUBIN, *op. cit.*, p. 69, n° 5.2.

de passe ou une clé de chiffrement. Ce mode d'authentification peut être couplé avec le mode d'authentification par la détention, exclusive d'une carte magnétique, par exemple. Des procédés de reconnaissance des caractéristiques biométriques d'un individu (cris, voix, empreintes digitales) plus récents permettent l'identification de la présence d'une personne lors d'une action. A eux seuls, ils peuvent difficilement constituer un procédé d'authentification dans la mesure où ils n'attestent pas de la volonté d'émettre comme sien un message.

L'authentification peut être résumée comme ceci : lors d'échanges d'informations entre deux acteurs, l'authentification permet à chacun de s'assurer que l'acteur avec qui il dialogue est bien celui qu'il prétend être.

Lorsque cela est établi, dans le cadre fermé d'un dialogue, les deux acteurs peuvent se faire confiance. Par contre, si l'on introduit un troisième acteur, ce type d'authentification peut ne plus suffire puisque les deux interlocuteurs peuvent mentir au troisième. L'émetteur peut prétendre qu'il a, ou n'a pas, envoyé un message au récepteur qui peut déclarer qu'il a reçu ou non un message, et cela indépendamment de ce qui s'est réellement passé. Quatre cas sont possibles, selon J. Hubin :

« 1. L'émetteur déclare avoir envoyé un message et le récepteur déclare l'avoir reçu : dans ce cas, aucune dispute.

2. L'émetteur déclare qu'il n'a pas envoyé le message et le récepteur dit qu'effectivement il n'a rien reçu : ici non plus, pas de problème en vue.

3. L'émetteur prétend ne pas avoir émis le message que le récepteur prétend avoir reçu. Dans ce cas, l'un des deux acteurs ment. Soit le récepteur a lui-même créé le message et essaie de faire croire qu'il provient de l'émetteur : on parle alors de forgery. Soit l'émetteur a effectivement émis le message mais en refuse la paternité : on peut alors parler de répudiation de l'origine.

4. Le récepteur assure ne pas avoir reçu le message que l'émetteur prétend lui avoir envoyé. Ici également on peut considérer qu'un des acteurs ment. Soit l'émetteur n'a pas envoyé le message mais essaie de le faire croire : on peut alors parler de falsification de l'émission. Soit le récepteur a bien

reçu le message mais nie en avoir jamais eu connaissance : il y a alors répudiation de la livraison ».

En d'autres termes, dès que l'on est dans un environnement où plusieurs intervenants étrangers et inconnus l'un à l'autre peuvent jouer (environnement ouvert) (27), les procédures d'authentification de l'auteur d'un message ne suffisent plus. Il faut que l'authentification porte à la fois sur le document et la signature de telle sorte que ce soit cet ensemble qui ne puisse avoir été produite que par la personne s'en prétendant l'auteur et ne soit lisible que par la ou les personne(s) autorisé(es) (28). Enfin, la vérification de l'authentification doit pouvoir être effectuée par tous les participants potentiels au réseau, en d'autres termes un registre des signatures doit pouvoir être accessible.

Les systèmes de cryptage permettent précisément cela. Par cryptage (ou chiffrement), on entend la transformation d'un message en clair en une chaîne de caractères alphanumériques dont la suite est incompréhensible sauf pour la personne autorisée à la déchiffrer. Le cryptage combine deux éléments :

— un algorithme (plusieurs algorithmes existent sur le marché : le DES, — Data Encryption Standard — créé dans les années 1960 par IBM, actuellement utilisé par le gouvernement américain ; le RSA (Rivest, Shamir et Adelman) mis au point en 1976, essentiellement destiné à conjurer les risques afférents au transport des clés sur les réseaux ; enfin, le PGP (Pretty Good Privacy) mis au point par Zimmermann disponible sur Internet et récemment autorisé par le gouvernement américain. Les algorithmes sont publics ;

— une clé sur laquelle « tourne » l'algorithme choisi. une clé est une chaîne de bits aléatoires, produite par un générateur de clés, d'une longueur variable, allant de 40 bits à 1024 bits, éventuellement ; plus la clé est longue, plus le message est difficile à décrypter. La longueur des clés est donc un enjeu hautement politique entre les Etats (29).

(27) On conçoit l'importance de cette exigence dans le cas d'un commerce électronique dans des réseaux largement ouverts, comme Internet, ou plus restreint, par ex. dans le secteur de l'assurance comme celui d'Assurnet.

(28) A cet égard, se trouvent également résolues les délicates questions de confidentialité des messages exigées notamment par les réglementations de protection des données (A cet égard, le rapport de l'OTA : US Congress, Office de Technology Assessment, Information Security and Privacy in Network environment, OTA-TCT-606 (Washington, DC : US Government Printing Office, Sept. 1994)

L'algorithme peut être asymétrique ou symétrique (30). En particulier le chiffrement asymétrique consiste en l'utilisation tant au moment du chiffrement que du déchiffrement de deux clés : l'une secrète, celle selon le cas, de l'émetteur ou du récepteur, l'autre publique, celle selon le cas de l'émetteur ou du récepteur (31). C'est le texte émis qui est chiffré grâce à la clé secrète de l'émetteur puis grâce à la clé secrète du destinataire. Le destinataire ne pourra déchiffrer le texte qu'en lui appliquant successivement sa clé secrète et la clé publique de l'émetteur. Ainsi, il sera l'auteur du message.

Une des questions essentielles est donc l'attribution des clés privées et « publiques » et le fait de porter ces dernières à la connaissance de tous. Cette fonction d'émission et de publicité des clés est le fait d'un certificateur. Ce certificateur joue un rôle comparable à celui d'un notaire. Il « authentifie » l'émetteur et le récepteur d'un message.

Ce notaire peut ne pas se borner (32) à ce premier rôle mais en outre offrir des services de sécurisation lors de l'échange de

(29) Pour des raisons d'efficacité, on ne peut imaginer signer le message complet. Dans ce cas, la signature serait souvent aussi lorsque le message. C'est pourquoi on utilise des « Hash Functions » (ou fonctions de compression). Ces fonctions ont pout but, quelque soit la longueur du message de les comprimer à une longueur donnée (par exemple, à 515 bits). C'est le message comprimé qui est signé. Pour vérifier la signature, le destinataire du message utilise alors la clé publique pour décrypter la valeur comprimée signée (le signed hash value). Si cette valeur correspond à celle obtenue en appliqaunt la même fonction de compression au texte complet du message, alors le message et la signature sont corrects. L'algorithme de compression est calculé de manière telle qu'il soit quasiment impossible de trouver deux messages avec le même résulté de compression.

(30) Dans les systèmes symétriques, l'émetteur et le destinataire utilisent la même clé secrète de cryptage, l'émetteur encrypte et le destinataire décrypte. Le système le plus utilisé est celui développé par IBM et standardisé depuis 1977. La cryptographie symétrique de par sa nature n'est applicable que dans des réseaux fermés.

(31) Le « Digital Signature Standard » (DSS) américain repris comme Federal Information Processing Standard (FIPS 186) approuvé par le National Institute of Standards and Technology (NIST) repose sur un système de cryptographie asymétrique à clé publique (à ce propos le rapport réalisé sur l'US Congress par l'OTA, Information Security and Privacy in Network environments, Congress of U.S., OTA-TCT-606 (Washington DC, U.S., Government Printing Office, Sept. 1994).

(32) « Indeed, the public keys need not be transmitted secretly but they have to be authentic. For this purpose, there have to be trusted third parties (TTPs). These are independant bodies without any vested interest in the system. The trusted third parties sign elctronically the name and the public key of a each participant. This is a certificate. In order to be sure about the authenticity of the public key of a participant one has to verify the signature of the TTP in the certificate. If this is successfull, then the public key is said to be authenticated. Evidently, for this purpose the public key of the TTP

messages. « Si un échange entre deux entités se fait par l'intermédiaire d'un réseau géré par une tierce personne et si cette personne est reconnue par les autres, elle peut enregistrer les messages émis par d'autres entités. Ce stockage pourra servir de preuve en cas d'arbitrage de conflit par la tierce personne de confiance. Dans un schéma de ce type, la signature est contrôlée par une autorité extérieure. Par analogie à la vie courante où dans ce cas on utilise un notaire, on parle de notarisation. Les schémas ainsi développés sont alors appelés schémas de signature avec notarisation » (33).

Nous reviendrons amplement sur le rôle assumé par les tiers certificateurs dans la troisième Partie solution institutionnelle. Ils constituent précisément ce que nous qualifions.

9. — *Les fonctions de la signature*. Pour ne reprendre que les deux fonctions (34) essentielles de la signature, à savoir l'identification de l'auteur d'un document (35) et la confirmation que l'auteur approuve la teneur dudit document (36), l'ar-

is necessary which has to be obtained from a trustworthy source. If there is e.g. only one TTP in a country, it would be easy to store its public key on each smart card issued, so that each participant in the system could verifiy a certificate with a key stored on his own card which hence is trustworthy« , (H. FARROUKH, B. HORNUNG, *New Dimensions for electronic Security in the development of Patient Card Systems*, not yet published.

(33) J. HUBIN, *op. cit.*, p. 78. Les notaires entendent bien jouer un rôle dans cette « notarisation électionique ». Ainsi, la proposition de la chambre fédérale allemande des notaires S. ERBER-FELLER, « Draft Bill of the German Federal Chamber of Notaries regarding the introduction of the Digital Signature », *EDI Law Rev.*, 3, (1996), n° 1.

(34) Sur ces deux fonctions de la signature, lire la note de M. VAN QUICKENBORNE, « Quelques réflexions sur la signature des actes sous seing privé », *R.C.J.B.*, 1985, pp. 57 à 104 et D. SYX, *Vers de nouvelles formes de signature ?*, Droit de l'inf., 1986, 3, pp. 135 et s.

(35) En d'autres termes, la relation « signature-signataire » doit être unique et absolue : à une signature donnée, on ne pourra associer qu'un et un seul signature. Toutefois, en ce qui concerne les documents informatiques, la vérification et l'adéquation entre la signature et le signataire ne peut plus être réalisée de façon visuelle comme c'est le cas pour la signature manuscrite. La vérification de la correspondance « texte-signature » est donc réalisée, non plus par une personne humaine, mais par des moyens informatiques appropriés (programmes...).

(36) « L'apposition de la signature doit être significative et se faire sur le document même auquel la signature se réfère. La signature doit y rester attachée de façon permanente et indissociable pendant le transport du document.

Il faut tout d'abord que l'acte de signature soit significatif. Cela revient à dire que le document doit être lisible et compréhensible et que la signature doit exiger une démarche volontaire de la par du signataire. Cette condition n'est pas nouvelle, elle est assez facilement réalisable tant au niveau du document papier 'classique' qu'au niveau du document 'informatique' (apparition sur l'écran de l'opération souhaitée avant de pousser sur la touche OK).

Par ailleurs la signature doit se faire sur le document auquel elle se réfère. Cette condition ne pose aucune difficulté pour les documents de type papier. En effet, la signature

ticle 6 du code CNUDCI édicte comme conditions de reconnaissance d'une signature électronique :

« *a*) a method is used to identify the originator's approval of the information contained therein ; and *b*) that method (37) is reliable as what appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any agreement between the originator and the adressee of the data message ».

10. — *Réflexions complémentaires.*

L'approche proposée indique clairement :

1) la nécessité d'une normalisation : la sécurité du commerce électronique exigera que les protocoles d'identification

apposée sur la papier n'est valable qu'au regard du contenu de celui-ci et n'est pas effacable. Pour respecter la condition selon laquelle l'apposition de la signature doit être faite sur le document même, il faut que, physiquement, le document et sa signature ne fassent qu'une seule unité de stockage sur le support informatique. Or tel n'est pas toujours le cas. En effet, il se pourrait que pour des raisons de calcul, de gestion ou de sécurité, les signatures aient besoin d'un niveau de privilège supérieur à celui donné aux documents (un privilège dans le cadre d'un système informatique est un moyen de protection des données qui représente le droit pour une personne à connaître des informations contenues dans ce système). Par conséquent, leur stockage aurait lieu sur différents supports et ce, malgré les liens logiques les unissant.

Peut-on en conclure que la signature n'est pas liée au document signé ? La réponse est négative et ce pour deux raisons. La signature électronique, par exemple, est par définition 'accolée au document' auquel elle se réfère et elle est 'établie en fonction du contenu du document'. Par conséquent, et bien qu'elle puisse en être distincte physiquement, la signature demeure dépendante logiquement du document.

Pour adapter la condition d'attachement permanent et indissociable de la signature aux 'documents informatiques', il faut utiliser des méthodes permettant de garantir l'inaltérabilité des documents. Dès lors, l'ajout, la modification ou la suppression d'une signature demeurera impossible », M. ANTOINE, M. ELOY, *op. cit.*, p. 67.

(37) Le rapport déjà cité du secrétaire général de l'UNICTRAL interprête comme suit la seconde condition : « Pour déterminer si la méthode utilisée en vertu du paragraphe 1 a) est appropriée, les facteurs juridiques, techniques et commerciaux à prendre en considération sont les suivants : 1) le degré de perfectionnement du matériel utilisé par chacune des parties ; 2) la nature de leur activité commerciale ; 3) la fréquence avec laquelle elles effectuent entre elles des opérations commerciales ; 4) la nature et l'ampleur de l'opération 5) le statut et la fonction de la signature dans un régime législatif et réglementaire donné ; 6) la capacité des systèmes de communication 7) les procédures d'authentification proposées par les opérateurs des systèmes de communication 8) la série de procédures d'authentification communiquée par un intermédiaire 9) l'observation des coutumes et pratiques commerciales ; 10) l'existence de mécanismes d'assurance contre les messages non autorisés ; 11) l'importance et la valeur de l'information contenue dans le message de données ; 12) la disponibilité d'autres méthodes d'identification et le coût de leur mise en ouvre ; 13) le degré d'acceptation ou de non-acceptation de la méthode d'identification dans le secteur ou domaine pertinent, tant au moment où la méthode a été convenue qu'à celui où le message de données a été communiqué ; et 14) tout autre facteur pertinent ».

et d'authentification soient fixés par des instances neutres et indépendantes ;

2) la reconnaissance d'exigences variables quant à la qualité des signatures, en particulier selon l'importance du message ;

3) la nécessité d'une définition ouverte, afin de permettre, en fonction des progrès techniques, des techniques de signature adaptées à ceux-ci (38). Cette dernière réflexion crée d'ailleurs un certain malaise clairement entrevu par les experts : la fabrication d'une clé réputée indéchiffrable il y a 10 ans peut être aujourd'hui au regard des progrès de la technologie un jeu d'enfants. Comment assurer dès lors la régénération des signatures (39) afin de maintenir leur sécurité ;

4) enfin, on notera une importante différence entre la signature manuscrite et celle électronique. La signature manuscrite est falsifiable ; celle électronique l'est difficilement voire jamais. L'usurpation de signature supposera presque toujours la négligence de son titulaire. Dans ce contexte, il est difficile de ne pas donner également à celui qui s'est fait « voler » sa signature électronique une certaine responsabilité voire, le cas échéant, une coresponsabilité pénale (40). Ce constat plaide pour la reconnaissance d'un mandat apparent de celui qui s'est laissé « voler » sa signature envers celui qui s'en est servi (41).

(38) A ce propos, l'introduction particulièrement éclairante du « Digital Signature Guidelines » de l'American Bar Association, Draft du 5 oct. 1995, qui explicitement, se réfère aux standards de l'ancienne ICCTT devenue International Telecommunications Union (ITU). A noter également que la loi de l'UTAH sur la signature digitale se réfère explicitement au Standard X.509 de l'ITU.

(39) Ainsi, ce principe du Computer Security Act américain de 1987 (P.L. 100.235) qualifié de Risk Based Standard « commensurate with the risk and magnitude of the damages resulting from the loss, misuse or unauthorized access to or modification of the information ».

(40) L'idée est avancée par le Committee ayant présidé à la réforme législative car la loi de l'UTAH et dont le rapport est publié partiellement dans l'*EDI Law Review* (1995, 2, 157 et s.).

(41) B. Amory et M. Schauss, *Concluding international contracts by electronic means, Formation of contracts : communications of the offer and acceptance to the offeror*, Institute of Int. business Law and Practice, Madrid, March 2-3, 1987, et les références reprises ; L. Elias et alii, « Le droit des obligations face aux échanges de données informatisées », *Cahier du CRID*, n° 8, Bruxelles, Story Scientia, 1991.

C. — *L'écrit électronique* (42)

11. — *L'écrit : un concept ouvert.* La notion d'écrit n'est guère définie par notre législation. La seule définition légale de l'écrit est celle du code de procédure civile allemand (43) ; le terme« écrit » recouvre toutes « les formes d'expression directement lisibles (44), qu'elles soient sur support papier, optique, magnétique, etc. » (45) Une telle définition confirmée par d'autres jurisprudences (46) répond au souci de rencontrer les procédés multiples et variés de stockage et de transmission de données.

La grande valeur probante reconnue à l'écrit s'explique par ses caractéristiques. Il constitue un support stable et fiable sur lequel figurent des signes lisibles formant un langage. Un tel concept est « ouvert » et son extension ne se réduit pas au seul document papier : le langage peut être codé et la lisibilité peut s'entendre de la possibilité pour le document d'être à tout moment produit, la stabilité et la fiabilité, enfin, peuvent être garanties par le mode technique de stockage et de transmission des signes et non par la qualité du papier. Bref, on reconnaît comme écrit tout document reproduisant de façon suffisamment durable la volonté d'une personne par des signes susceptibles d'être lus, grâce à un procédé approprié et non seulement l'apposition sur papier de signes. On ne s'étonnera pas dès lors de l'audace de l'Administration fiscale française qui, en matière de facture créée et transmise électroniquement reconnaît : « en cas de télétransmission, la valeur probante des documents échangés dépend essentiellement de l'instauration

(42) Cf. à ce propos le préambule de l'EFT Regulation proposé par la Federal Reserve System (publié in Fed. Register 61, n° 86, 2 mai, 1996). « A writing up to present, has typically been presumed to mean a paper document... information that is produced, stored or communicated by computer too is generally considered to be a writing,... these documents are considered written documents when kept in electronic form as well as when printed on paper ».

(43) Z.P.O. (Code de procédure civile), § 415 f.

(44) Par « directement lisibles », on entend que le système soit capable de reproduire l'information quasi instantanément et dans une forme directement lisible.

(45) A noter à cet égard le rapprochement des définitions données par l'Uniform Commercial Code (UCC) la première en 1947, la seconde en 1976 de la notion de « Writing ».

(46) Ainsi, en particulier la jurisprudence française déjà ancienne sur l'article 1347 du code Napoléon qui a propos du commencement de preuve par écrit, admet l'enregistrement sonore, la photographie, etc... Cf. dans le même sens, les doctrines et jurisprudences néerlandaise, luxembourgeoise, portugaise et irlandaise (cf. I. De Lamberterie (éd.), rapport cité, p. 57).

d'un dispositif technique assurant au système une fiabilité équivalente à celle que procure l'impression des factures sur papier et permettant d'assimiler la facture transmise par voie télématique à un original » (47).

12. — *Du document électronique à l'écrit* : trois qualités fonctionnelles (48) caractérisent l'écrit et justifient la valeur probante supérieure de celui-ci : l'inaltérabilité, la lisibilité et la stabilité. Ces qualités doivent être requises d'un document électronique qui souhaite se voir reconnaître le statut d'écrit :

— le document doit être **inaltérable** : parler d'inaltérabilité d'un document, c'est évoquer les fraudes. Alors que sur les supports papier, celle-ci est assez facile mais très rapidement remarquée (« gratter » et/ou recopier une information laisse des traces), la fraude sur un support informatique passe souvent inaperçue et ne peut presque jamais être détectée *a posteriori*.

Préserver le caractère inaltérable d'un document nécessite de conserver celui-ci inchangé à la fois dans son contenu ainsi que dans sa forme.

Pour assurer l'inaltérabilité du document dans son contenu (c'est-à-dire pour préserver le sens et le caractère authentique du document original), il faut que l'émetteur et/ou le récepteur ne puissent modifier le contenu du document à l'insu de l'autre partie (ainsi, la modification d'un texte n'entraînerait-elle pas modification de la signature). De plus, il faut qu'un

(47) Instruction fiscale du 27 décembre 1991, prise en application de l'article 47 de la loi de finances rectificative. Sur cette question, Th. PIETTE-COUDOL, *l'EDI et le droit*, Ed. Hermès, Paris, 1991.

(48) Lors de l'élaboration de la Loi type, une attention particulière a été accordée aux fonctions traditionnellement assurées par divers formes d'« écrits » sur papier. C'est ainsi par exemple que la liste non exhaustive ci-après indique les raisons pour lesquelles la législation nationale exige la présentation d'« écrits » : 1) veiller à ce qu'il y ait des preuves tangibles de l'existence et de la nature de l'intention manifestée par les parties de se lier entre elles ; 2) aider les parties à prendre conscience des conséquences de la conclusion du contrat ; 3) fournir un document lisible par tous ; 4) fournir un document inaltérable et conserver en permanence la trace d'une opération ; 5) permettre la reproduction d'un document de manière que chaque partie ait un exemplaire du même texte ; 6) permettre l'authentification des données au moyen d'une signature ; 7) assurer que le document se présente sous une forme acceptable par les autorités publiques et les tribunaux ; 8) consigner l'intention de l'auteur de l'écrit et conserver la trace de cette intention ; 9) permettre un stockage aisé des données sous une forme tangible ; 10) faciliter le contrôle et les vérifications ultérieures à des fins comptables, fiscales ou réglementaires ; et 11) établir l'existence de droits et obligations juridiques dans tous les cas où un «écrit» était requis aux fins de validité » (rapport du secrétiare général de la CNUDCI, *op. cit.*, n° 58.).

tiers ne puisse pas interférer dans les relations émetteur-récepteur en modifiant le contenu du document à l'insu des parties.

Diverses techniques d'authentification des documents (*supra*, n° 8) permettent de garantir l'intégrité des données.

— le document doit demeurer **lisible** : les documents sur papier remplissent directement cette condition par le simple fait qu'ils sont rédigés dans un langage (vocabulaire et grammaire) et dans une symbolique graphique (écriture) accessible à la compréhension humaine. Tel est le cas des informations reprises sur support informatique : Certes elles y sont codées et se trouvent donc sous forme illisible, mais il est possible d'avoir recours à un intermédiaire « approprié » qui présentera les données stockées sous une forme compréhensible par l'homme.

La Regulation E proposée par le Board of Governors du Federal Reserve System (49) à propos des transferts électroniques de fonds réclame cette qualité du système pour que celui-ci puisse prétendre émettre des documents électroniques ayant valeur d'écrit même s'il reconnaît que cette exigence n'est pas simple à rencontrer lorsque le client émetteur d'ordres est un consommateur ne disposant pas des outils nécessaires à la lecture : « The Board believes that the requirement for clear and understandable disclosures applies fully to electronic communications » (50).

— Le document doit être **stable** : la stabilité du document papier est évidente puisque le support se dégrade peu. En matière électronique, la condition est plus délicate à remplir : a la fois, les informations circulent aisément d'un support à l'autre mais pire, les supports de stockage (bande magnétique, CD ROM, disque optique) connaissent une obsolence rapide et toute modification de configuration oblige souvent à des retranscriptions.

(49) Electronic Fund Transfers, Fed. Re. Systems 12 CFR Part 205, Reg. E, Docket n° R.0919, Fed. Register, 61, n° 86, Thursday May 2, 1996.

(50) Cf. également les réflexions de l'UNICTRAL à ce propos : « Le mot 'accessible' implique qu'une information se présentant sous la forme de données informatisées doit être lisible et interprêtable et que le logiciel qui pourrait être nécessaire pour assurer la lisibilité de pareille information doit être préservée » (rapport cité, n° 60).

13. — *de l'écrit à la copie « fidèle »*. Comment la preuve électronique peut-elle rencontrer cette exigence ? Deux réflexions nous apparaissent essentielles à ce propos : la première consiste à lever une ambiguité (51) : la stabilité du document s'entend plus d'une garantie de perennité du contenu et non du support dont la régénération peut être multiple. La législation Québécoise a parfaitement bien compris la nécessité de ce glissement lors de sa réforme récente du droit de la preuve. Deux articles, les articles 2837 et 2838, précisent :

article 2837 « Lorsque les données d'un acte juridique sont inscrites sur support informatique, le document reproduisant ces données fait preuve du contenu de l'acte, s'il est intelligible et s'il présente des garanties suffisamment sérieuses pour que l'on puisse s'y fier. »

article 2838 « L'inscription des données d'un acte juridique sur support informatique est présumée présenter des garanties suffisamment sérieuses pour que l'on puisse s'y fier lorsqu'elle est effectuée de façon systématique et sans lacune, et que les données inscrites sont protégées contre les altérations. Une telle présomption existe en faveurs des tiers du seul fait que l'inscription a été effectuée par une entreprise ».

Comme le relève Mr. Piette-Coudol (52), de telles expressions témoignent du fait que l'attention est portée sur le contenu de l'acte et non sur son support.

La seconde réflexion consiste à changer les mentalités et à abandonner l'approche habituellement jetée sur la copie, approche avalisée par la loi par son article 1334 du code civil (53).

Les sécurités techniques et organisationnelles qui peuvent entourer les opérations d'archivage électronique plaident pour

(51) Reprendre la réflexion d'I. DE LAMBERTERIE, *op. cit.*, p. 682 : « Que veut dire 'inaltérable', 'durable' ?. On ne trouve aucune interprétation jurisprudentielle de ce terme et les définitions proposées ne sont pas équivalentes : pour certains, inaltérables veut dire que l'on ne peut pas modifier le document, pour d'autres cela veut dire qu'il n'a pas été modifié ».

(52) Th. PIETTE-COUDOL, *EDI, Trois niveaux de contrats, trois systèmes de preuve, Expertises*, mai 1993, p. 178. Il est à noter que la loi québécoise s'inspire grandement des travaux remarquables réalisés par MM. P. TRUDEL, G. LEFEBVRE et S. PARISIEN publiés sous le titre, *Etude sur les enjeux juridiques des échanges de documents informatisés*, Montréal, Thémis, 1993.

(53) A cet égard, J.P. BUYLE, « Nouvelles règles en matière de preuve par copie de documents », *J.T.*, 1993, p. 197 et les nombreuses références y reprises.

un changement de mentalités. La distinction « original-copie » y répond non seulement aux besoins soulevés par l'archivage, c'est-à-dire la conservation à plus long terme des données mais également à l'exigence de tenir compte de l'intrinsèque volatilité des documents électroniques transmis instantanément d'une mémoire à l'autre pour les besoins de la transaction voire par les seules nécessités du système. En d'autres termes, en matière de document électronique, il est difficile de distinguer l'original de sa copie et l'opprobre lancée par quelques législations sur les copies soulève difficultés. La nécessité de reconnaître à la copie fidèle la même force probante que l'original répond à cette inquiétude exprimée par les entreprises dans leurs relations tant avec leurs clients et leurs fournisseurs qu'avec les administrations. Si modification législative il doit y avoir, c'est à propos de la valeur probante des modes de conservation des transactions et non des modes de conclusion de celles-ci.

La notion de copie est donc à définir : « constitue une copie, le document reproduit sur support d'informations provenant de l'enregistrement d'un écrit sous signature privée » et le qualificatif « fidèle » de même. Une copie est réputée fidèle lorsque les originaux ont été enregistrés selon des critères de sécurité fixés par l'autorité, c'est-à-dire des critères d'intégrité et, le cas échéant, de durée et de confidentialité.

Notre définition mettant l'accent sur la nécessité de la fidélité de la copie et le respect de règles de sécurité assurant cette fidélité rejoignent l'exigence québécoise de « garanties suffisamment sérieuses pour que l'on puisse s'y fier », affirmée par l'article 2838 du code civil québécois. On sait que le Conseil de l'Europe a émis à cet égard des recommandations (54) précisant les qualités techniques et organisationnelles nécessaires pour procéder à une copie fidèle électronique.

Le respect de ces exigences et de ces critères doit être total. Nous ne pouvons admettre la solution trop libérale de récentes

(54) Recommandation du Conseil de l'Europe, n° R (81) 20, « relative à l'harmonisation des législations en matière d'exigence d'un écrit et en matière d'administration de reproduction de documents et des enregistrements informatiques (publié notamment in Lamy, Droit de l'Informatique, 1995, n° 2306).

lois belges (55) autorisant certaines entreprises à prouver par copie (56) pour autant que la confection de cette copie ait été faite sous leur responsabilité. La loi ne donne aucune règle sur les modes d'établissement des copies et le Roi, autorisé à les fixer, n'a pris aucune décision à ce jour (57).

DEUXIÈME PARTIE. — Le cadre conventionnel du commerce électronique les EDI agréements

A. — *Préliminaires*

14. — *une définition de l'accord d'interchange.* L'accord de transferts électroniques de données (Electronic Data Interchange) peut se définir comme « un contrat cadre » (58) par lequel deux ou plusieurs personnes, physiques ou morales, établissent les conditions juridiques et techniques d'utilisation de leur échange de données informatisées (59) dans le cadre de leurs relations commerciales (60). Sous l'impulsion de multiples organisations privées (61) ou publiques, sectorielles ou non, se sont multipliés des accords modèles dits d'Interchange (62). Cette multiplication devait conduire la Commission européenne à recommander le 19 octobre 1994 un accord type d'Interchange (63) dont le contenu sera analysé ci-après et la Commission des Nations Unies pour le droit du commerce international (CNUDCI) à élaborer une « loi type sur certains aspects juridiques de l'échange de données informatisées et des moyens connexes de communications » ainsi qu'un guide pour son incorporation (64). Il s'agit par ces divers moyens de « promouvoir l'échange de données informatisées en fournissant un moyen concret et souple d'aborder les questions juridiques soulevées par son utilisation et en encourageant les utilisateurs à coopérer pour s'échanger des messages EDI » (65).

15. — *Au-delà des accords d'interchange.* Outre cet accord d'Interchange, les milieux concernés ont élaboré sur le modèle des INCOTERMS, des EDITERMS (66) c'est-à-dire des données juridiques, c'est-à-dire d'ajouter aux indications techniques et commerciales, certaines indications sur la portée juridique de tel ou tel message (ainsi indiquer qui a la responsabilité du transport de la marchandise objet de la convention

(55) Il s'agit de l'article 196 de la loi du 17 juin 1991 (*M.B.*, 9 juillet 1991) à propos des établissements financiers sociétés anonymes de droit public, de l'article unique de la loi du 22 juillet 1991 (*M.B.*, 6 sept. 1991) à propos des établissements bancaires et d'assurances et de l'article 95 de la loi du 28 juillet 1992 (*M.B.*, 31 juillet 1992) à propos d'autres intermédiaires financiers.

(56) Les copies selon les textes cités, font foi comme les originaux dont elles sont présumées, sauf preuve contraire, être une copie fidèle. Bref, l'entreprise se trouve dispensée de toute preuve de la fidélité de la copie.

(57) Pour une critique des textes légaux, lire J.P. Buyle, *art. cité*, p. 200.

(58) Contrat-cadre qui curieusement se concluera par écrit. Il constitue en quelque sorte « l'ultime trace écrite » (L. Costes, « Vers un droit du commerce international sans papier », *R.D.A.I.*, 1994, 6°, p. 741).

(59) L'EDI et le message EDI définis par l'accord type européen (cf. *infra*, note 47) comme suit :

EDI : L'échange de données informatisées est le transfert électronique d'un ordinateur à un autre, de données commerciales et administratives sous la forme d'un message EDI structuré conformément à une norme agréée.

Message EDI :

Un message EDI est un ensemble de segments structurés selon une norme agréée, se présentant sous forme permettant une lecture par ordinateur et pouvant être traitées automatiquement et de manière univoque.

(60) E. Caprioli, « Les accords d'échange de données informatisées », *Cahiers Lamy*, mai 1992 (C), p. 6. Sur les accords d'interchange, en Belgique lire L. Elias, J. Gérard, GK. Wang, « le droit des obligations face aux échanges de données informatisées », Story Scientia, *Cahier du CRID*, n° 5, Bruxelles, 1992 ; S. Katus (éd.), *EDI in Belgie*, die Kleure, 1993 ; M. Antoine, J.F. Brakeland, M. Eloy, *Le droit de la preuve face aux nouvelles technologies de l'information*, Story Scientia, *Cahier du CRID*, n° 4, Bruxelles, 1992. De manière générale, l'excellent ouvrage de B.D. Reams, C.J. Kutten, A.E. Strehler, *Electronic contracting law*, CBC, Deafild, 1992, 93.

(61) Ainsi la CCI, qui dès le 22 septembre 1987 édictait des règles de conduite uniformes pour l'échange de données commerciales par télétransmission.

(62) Sur une liste complète, R. Van Esch, « Interchange Agreements », *EDI Law Review*, 1994, 1, pp. 3-41 ; Cf. également R. Blechschmidt, « The German basic Electronic Data Interchange Agreement versus the European Model Agreement. Two different options for trading partners in an EDI environment », article à paraître in *EDI Law Review*.

(63) Recommandation de la Commission CE du 19 octobre 1994 concernant les aspects juridiques de l'EDI (*J.O.C.E.*, 28 déc. 1984, n° L 338, p. 38). Cette recommandation est reprise en annexe.

(64) Sur l'ensemble des travaux de la CNUDCI, lire le rapport du Secrétariat général à propos du Guide pour l'incorporation de la loi type de la CNUDCI sur certains aspects juridiques de l'EDI et des moyens connexes de communication, A/CN/9/426, 24 avril 1996.

(65) selon les termes mêmes du préambule de la recommandation européenne.

(66) Cette notion rebaptisée ETERMS par les travaux de la CCI (Working Party on the Legal Aspects of Electronic Commerce — voir le compte-rendu de la réunion du 28 nov. 1995) a été développée par des auteurs français (cf. A. Bertrand, « Le contrat d'interchange dans une perspective historique : vers des Incoterms, EDI » in *Le nouveau droit des EDI*, p. 107 et E. Caprioli, « Les limites des accords d'EDI : la solution des Editerms », *Cahiers Lamy*, Juillet 1993, (E.), pp. 10 et s. « To facilitate electronic commerce, the ETERMS project seeks to make publicly available a data base which contains legal terms that can be referred to by means of a unique identifier. Specific legal terms are incorporated in an electronic message by reference to the specified ETERMS (CCI, ...) ».

EDI ou le cas échéant une réserve de propriété à son propos. La notion de « profil d'interchange » proposé par Th. Piette-Coudol (67) est plus ingénieuse encore. Il s'agit, selon son auteur, « d'un scénario juridique préétabli associant harmonieusement des éléments juridiques, techniques et sécuritaires en relation avec une relation déterminée ». En d'autres termes, il s'agirait pour les parties en intégrant la référence idoine au profil choisi (68), de régler plusieurs questions juridiques relatives à l'échange de données informatisées et aux conséquences de la transaction électronique ainsi initiée.

B. — *De quelques dispositions de l'accord type européen* (69)

16. — *Objet de l'accord.* L'objet de l'accord porte uniquement, précise l'article 1.1, sur les termes et conditions légales qui s'appliquent aux parties effectuant des transactions par EDI mais non, ce qui serait l'objet des EDITERMS, la réglementation des transactions effectuées par l'EDI. En d'autres termes, des questions telles que la responsabilité du fournisseur ou de l'acheteur d'une marchandise objet d'une transaction EDI le transfert de sa propriété ou des risques, n'est pas réglée par l'accord EDI mais doit être réglée, de manière complémentaire à la souscription de l'accord type européen, par les EDITERMS appelés aussi profils d'interchange.

Une annexe technique s'ajoutera à l'accord d'interchange, elle précisera les spécifications nécessaires à l'opération souhaitée par les parties (structure du message, critères d'identification).

(67) Cet auteur a présenté son projet à plusieurs reprises à la CCI.

(68) Il s'agirait d'ajouter au message EDI, un segment identifiant le profil.

(69) Nous n'avons abordé que les regles relatives à la formation et a la preuve du contrat, nous n'avons pas analysé les règles relatives a la protection des données (a ce propos lire not. J. DUMORTIER, « Privacybescherming by EDI », in *EDI in Belgie*, S. KATUS (ed.), Die keure, 1993 et l'étude réalisée en 1995 et 1996 par l'Universite des Baléares et le CRID pour TEDIS, étude en voie de publication. De même, les questions relatives à la concurrence et à la responsabilite n'ont pas ete reprises. A cet egard, lire L. ELIAS, J. GÉRARD, G.K. WANG, *op. cit.*

Nous ne nous attarderons pas à l'article 2 qui énumère les définitions générales de l'EDI du message EDI, du répertoire UN/EDIFACT (70), et de l'accusé de réception.

17. — *Validité et force probante de l'accord EDI.* L'article 3 dans ses paragraphes 1 et 2. règle les problèmes délicats de la validité du contrat conclu par EDI. Ce premier alinéa propose une renonciation expresse de la partie à l'accord EDI de contester la validité de la transaction du seul fait qu'il a été effectué par voie électronique, ce qui pourrait s'avérer contraire aux règles nationales supplétives sur la validité d'un contrat ou sa force obligatoire. La contrariété du contenu avec des règles nationales impératives (ainsi, l'exportation de denrées interdites, le non respect de formalités imposées pour des opérations particulières (par ex. des opérations nécessitant l'intervention d'un notaire) oblige la partie au courant de cette contrariété à informer l'autre partie de cette incompatibilité. L'article 3.3. concerne le moment et le lieu où un contrat est conclu ou formé. Les conclusions d'une étude doctrinale (71) ont amené la Commission à accepter la règle de la réception déjà préconisée par la convention de Vienne sur la vente internationale de marchandises pour les contrats à distance. Cette règle fixe la formation du contrat au moment où le message EDI est reçu par l'ordinateur ou plutôt le système d'informa-

(70) Règle de syntaxe de l'UN.EDIFACT.ISO 9735 EN 9735, TDED UN/EDIFACT ISO 7372-EN 27372. L'UNTDID (répertoire d'échanges de données commerciales des Nations Unies contient également des lignes directrices à la conception des messages UN.EDIFACT, les lignes directrices relatives a l'exploitation de la syntaxe, un répertoire d'éléments de données, une liste de codes, un répertoire d'éléments de données composées, un répertoire des segments, un répertoire d'UNSM et les règles UNCID.

(71) A ce propos, les réflexions de L. ELAIS publiées in L. ELIAS, J. GÉRARD, G.K. WANG, *op. cit.* A noter la formule différente du modèle allemand. Le contrat est conclu « upon acknowledgment ». Cette formule est défendue par R. BLECHSCHMIDT (*art. cité*, note 46). Le modèle allemand distingue en effet les différents cas de communication EDI, soit les parties se transmettent le message d'un systeme d'information à l'autre, soit le système d'information du récepteur va rechercher le message dans le système d'information de l'emetteur ; soit le message est déposé dans une boîte par un réseau à valeur ajoutée et qui doit être relevée par le récepteur. Le système de l'accusé de réception renvoyé à l'émetteur et non de la réception est préférable, selon cet auteur, dans tous les cas.

tion (72) de l'offrant même si celui-ci n'en a pas encore pris connaissance.

L'article 4 affirme la recevabilité des messages EDI devant les tribunaux dans la mesure où le caractère supplétif des législations sur la preuve ou le contenu de ces législations lui-même (système de preuve libre) le permettent. La valeur probante de ces messages est également proclamée, elle n'est pas absolue mais entraîne un renversement de la charge de la preuve. Comme le note le commentaire de la Commission, « pour que l'EDI constitue une solution de remplacement aux transactions sur papier, il est essentiel d'accorder aux messages EDI, une valeur comparable à celle des documents utilisés jusque là ».

L'article 4.2. prend soin d'ajouter que cette recevabilité et cette valeur probante sont liées au respect des règles de sécurité qui sont détaillées aux articles suivants, en particulier à l'article 6 (73).

L'article 6 énonce l'obligation d'assurer un « niveau satisfaisant de sécurité des messages ». Ce niveau dépendra de l'importance de la transaction. La sécurité concerne tant les risques d'accès non autorisé, de modification, de distinction ou de perte du message. Elle consiste en des mesures permettant d'assurer la vérification de l'origine et de la destination du message. Ce sont essentiellement des techniques de chiffrement qui permettent d'assure une telle identification. Les mesures de sécurité doivent également vérifier l'intégrité du message.

Au cas où l'utilisation des procédures de sécurité conduisent au rejet d'un message EDI à la détection d'une erreur, le destinataire en informe l'émetteur et ne peut donner suite au message sauf autorisation de celui-ci.

(72) La notion de « système d'information » est large. Elle comprend selon les « Guidelines for the security of Information Systems » publiées en novembre 1992 par l'OCDE « Computers, communication facilities, computers and communication networks and data and information that may be stored, processed, retrieved or transmitted by them, including programs, specifications and procedures for their operation, use and maintenance ».

(73) La solution est la même selon le modèle allemand. La doctrine en effet ne considère pas qu'un message électronique est un document bénéficiant d'une présomption devant le juge mais que selon la procédure de preuve par inspection, sa valeur probante doit faire l'objet d'une évaluation par le juge (W. KILIAN et al., *Electronic Data Interchange (EDI), aus ökonomischer und juristischer Sicht*, Baden Baden, 1994, pp. 138 et s.). Le modèle prévoit cependant que si le mode de confection du message répond à certaines exigences, il devient un electronic document ayant une valeur égale au document papier (a ce propos, R. BLECHSCHMIDT, *art. cité*).

18. — *Traitement et conservation des messages EDI*. L'article 8 a trait au traitement des messages EDI (74). L'importance d'un traitement rapide des messages EDI est soulignée par l'article 5.1. Si un accusé de réception est requis par les parties, cet accusé de réception doit être envoyé rapidement (un délai de 1 jour ouvrable). La non réception de l'accusé attendu permet à l'expéditeur du message de le considérer comme nul et non avenu ou de tenter de le récupérer.

Ainsi, dans leur convention, les parties devront classer à l'avance les transferts en trois catégories :

— ceux qui ne nécessitent aucun acte du destinataire car ils sont de peu d'importance ;

— ceux qui nécessitent un accusé de réception (l'expéditeur veut s'assurer que le destinataire a pu prendre connaissance du message) ;

— ceux qui sont soumis à la technique de l'écho (l'expéditeur veut s'assurer que le destinataire a eu une parfaite et correcte connaissance de certains éléments (date, prix, ...). Ceci se justifie par le fait que ces éléments pourraient être déterminants pour la conclusion d'une transaction.

La conservation des données EDI est abordée à l'article 6. Assurer un transfert parfait n'est pas suffisant dans la mesure où si un litige éclate, la conservation d'un moyen de preuve s'avérera nécessaire. Une obligation de conservation est mise à charge des deux parties qui tiendront un registre chronologique et complet de toutes les transactions effectuées. L'inaltérabilité du contenu des messages lors de ces opérations de conservation doit être assurée (75).

(74) qui devront correspondre aux normes, recommandations et procédures UN/EDIFACT et reprendre les codes correspondant aux listes de codes développés et mis à jour par l'UN/EDIFACT dans la mesure ou ceux-ci existent.

(75) Cf. a cet égard nos réflexions dans la 1re partie, n° 8. Les règles UNCID insistent sur la nécessité de désigner nommément une personne, responsable de ces opérations.

TROISIÈME PARTIE. — UNE SOLUTION « INSTITUTIONNELLE : LES TRUSTED THIRD PARTIES » (TTP) OU TIERS CERTIFICATEURS (76)

19. — *Le contexte — les fonctions des T.T.P.* Le commerce électronique a été jusqu'à présent le fait de sociétés ayant des relations continues et intenses (77). Le développement remarquable et la popularité d'Internet modifie de manière fondamentale les exigences en matière de signature électronique. Dans un réseau ouvert, international, « des algorithmes de signature standardisés, publiquement accessibles sont nécessaires » (78). En effet, l'absence de connaissance préalable du contractant requiert que l'on puisse être certain de son identité et que le contenu de la transaction puisse bien être authentifié comme le sien.

L'idée a été de recourir à des « certification Authorities », c'est-à-dire à des entités « investies (entrusted) par un ou plusieurs utilisateurs du pouvoir de créer et délivrer des certificats » (79). Un « certificat » est une structure de données signées digitalement qui lie le nom d'une entité avec sa clé publique (80). Pourvu ainsi d'une clé publique et d'une clé secrète, comme il a été expliqué plus haut à propos de la cryptographie asymétrique à clé publique (*supra* n° 8), l'émetteur d'un message peut le signer (81) c'est-à-dire transformer le message de manière infalsifiable tout en rendant possible pour le récepteur, à la fois la preuve de la source du message et l'intégrité de ce dernier (82). Certes, on peut imaginer d'autres objets de certification électronique ainsi la valeur de crédit d'une entité, la présence d'un témoin lors du passage d'un acte (83), la date d'existence d'un document (84).

(76) On parle également de « notaires électroniques ».

(77) Ce qui en particulier caractérisent les relations EDI, comme le notent REAMS, KUTTEN et STREHLER (*op. cit.*, p. 6) : « ... it usually has only been conducted between parties with close, long standing and continuing business relations ships ».

(78) Green Paper on the Security of Information Systems, Draft 3.6., p. 25 ; cf. également les réflexions de ANDERSEN, *art. cité*.

(79) C'est la définition donnée par l'I.T.U. X 509 § 3.3. (1993).

(80) Eod. loco. Cf. également la définition de l'American National Standards Institute (ANSI) X 9-30-199X « the public key and identity of an entity together with some other informations, rendered unforgeable by signing it with the private key of the certifying authority which issued it ».

(81) A propos de la signature électronique à clé publique, M. BAUM, *The proposal digital signature Standard : implications for electronic commerce*, CLSR (1992), 8, pp. 217 et s.

Le premier rôle des tiers certificateurs ou « trusted Third Parties » combine souvent la « nomination » c'est-à-dire la reconnaissance de la capacité d'une personne identifiée à bénéficier des services de certification et la « certification », c'est-à-dire l'attribution aux personnes « nommées » de leur nom et de leur adresse à une entité de la fonction de validation c'est-à-dire l'attestation d'une correspondance entre un nom, une adresse (électronique) et une clé publique. Le second rôle concerne la gestion des clés publiques et privées, c'est-à-dire la remise de clés et leur renouvellement, en même temps que la mise à disposition et la gestion d'un registre de clés. D'autres rôles peuvent lui être assignés (85), ainsi la gestion du réseau par lequel transiteront les messages, leur estampillage, leur stockage voire le rôle d'arbitrage entre les parties (86).

L'ensemble de ces rôles nécessite un contrôle strict de la qualité technique et opérationnelle des certificateurs et l'affirmation de leur responsabilité, ainsi au cas où il validerait un message dont la signature dont la signature a été répudiée par son prétendu auteur, au cas où des erreurs d'adressage apparaîtraient, etc.

(82) On connaît toutes les difficultés soulevées dans les différents pays en particulier aux Etats Unis par l'utilisation de tels procédés cryptographiques qui permettraient l'utilisation illicite des réseaux sans possibilité de contrôle pour l'Etat. Sur ces questions, lire not. l'excellent rapport de M. BAUM, *Federal Certification Authority : liability and policy, Law and policy of certificate based public Key and digital signatures*, U.S. Department of Commerce, N.T.I.S., June 94, Sur le même débat en Belgique, lire M. ANTOINE, « La cryptographie en droit belge », *Rev. dr. comm.*, 1996, à paraître.

(83) On parle alors de « transactional certificates ». Sur ces divers rales, cf. le Green Book de la Commission, Version 3.6., pp. 35 et s. A ce propos, on imagine bien le rôle d'un notaire électronique témoignant de sa présence lors d'une transaction.

(84) A propos de ces fonctions particulières, lire A.M. FROOMKIN, *The essential role of Trusted Third Parties in Electronic Commerce*, 75 Gregon L. Rev. 49 (1996) ; M. ANTOINE (« La certification », *Rev. dr. Comm.*, 1995, 4-14), développait ainsi l'idée d'un envoi électronique recommandé.

(85) Ces deux rôles peuvent être confiés à un opérateur ainsi le réseau ISABEL créé par le secteur bancaire belge et conçu comme un système standardisé de communication permettant des liaisons télématiques sécurisés entre partenaires, ne prend pas en charge la première fonction, à savoir la nomination du « subscriber » mais la remise de certificat et l'ensemble des autres rôles.

(86) Sur ces divers rôles, cf. le Green Book de la Commission, Version 3.6., pp. 35 et s.

20. — *La loi de l'UTAH, une première.* Si ces questions sont à peine naissantes en Europe, une attention particulière leur est accordée aux Etats-Unis (87). L'Utah a été le premier Etat à proposer ainsi une loi générale sur la signature électronique (88). Selon la loi, les documents signés électroniquement sont valables de la même manière qu'un document papier (89). Les conditions de reconnaissance de cette signature électronique sont nombreuses : le système de doubles clés asymétriques émis par une « certification authority » ayant reçu à cet effet une licence est nécessaire. Nombre d'obligations sont mis à charge de cette autorité en termes de capacité financière, d'indépendance et d'assurances. La loi d'Utah interdit en particulier à ces autorités de se comporter d'une façon telle qu'elles créent un risque commercial déraisonnable aux personnes qui fondent leur confiance sur les certificats émis. Les procédures de délivrance des certificats sont soigneusement décrits.

Conclusion

21. — *Réflexions finales.* Les développements jusqu'ici tenus autorisent les conclusions suivantes :

1. Le droit de la preuve des actes juridiques est en singulière évolution. Non dans les textes. Les concepts d'« écrit » et de « signature » à les regarder de près, s'adaptent merveilleusement aux techniques modernes de communication et de conservation des messages. Il s'agit au-delà des techniques ou

(87) Sur les diverses réglementations existantes aux Etats Unis lire P.R. Katz et A. Schwartz, *Electronic Document and digital signatures : changing the way business is conducted and contracts are formed*, IPC newsletter, 1996, 14, 2, pp. 3 et s. Cf. également les Digital Signature Guidelines émises par l'American Bar Association, fin 1995.

(88) La loi de l'Utah (Utah Digital Signature Act) date de 1995 et a été intégralement publiée par l'EDI Law Review, 1995, 2, 157-196. Un projet de loi (Signaturgesetz [Sig. G]) a été déposé au Parlement allemand, le 19 août 1996. Il contient les rubriques suivantes (trad. anglaise) : § 1er Object and Scope, § 2 Definitions, § 3 Licensing of Certificate Authorities, § 4 Issuance of Certificates and Time-stamps, § 5 Duties of Certificate Authorities, § 6 Contents and Expiration of a Certificate, § 7 Expiration of a Digital Signature, § 8 Suspension of a Certificate, § 9 Documentation, § 10 Bankruptcy of a Certificate Authority, § 11 Data Protection, § 12 Supervision of Certificate Authorities, § 13 Technical Devices, § 14 Recognition of Foreign Certificates, § 15 Further Regulations.

(89) « A valid digital signature verified using a public key is presumed to have been affixed with the intention of the subscriber to authenticate the message and to be bound by the contents (thereof...). A digitally signed document is as valid as if it had been written on paper » (§ 22, Utah Digital Signature Act).

supports auxquels on les a parfois confondu, d'analyser la fonction de ces concepts et de s'apercevoir que ces fonctions peuvent parfaitement être remplies par des documents ou signatures électroniques.

2. La convention d'échange de données informatisées présente entre partenaires une solution élégante, adaptable aux besoins particuliers à toutes les questions soulevées par la conclusion d'une opération par voie électronique. La normalisation y est essentielle et le respect des procédures fixées est essentiel pour assurer la confiance des parties et l'efficacité de la procédure électronique choisie.

3. L'émergence de réseaux largement ouverts conduit à relancer le débat sur la signature. La signature doit être reconnue non vis-à-vis d'un opérateur bien connu de l'auteur de la signature mais vis-à-vis de tiers indéterminés rencontrés au hasard des multiples navigations. Seules des autorités agissant comme intermédiaires pourront certifier un message qui doit nécessairement aboutir, et ne pouvoir être lu que par la seule personne habilitée. Dans ce contexte, la signature électronique réclame de nouvelles exigences : l'identification ne peut être que le fait d'un tiers dans la mesure où non connu *a priori* l'auteur d'un message pourrait revêtir de fausses identités ; l'authentification réclame que contenu du message et signature soient indissociables sous peine de risquer mille transformations du message au gré de son voyage sur le réseau. Bref, la signature n'est plus le seul fait de son auteur, elle doit nécessairement être « reconnue », « certifiée », « notariée ».